Descriptor Cache: Revealing The Hidden Registers

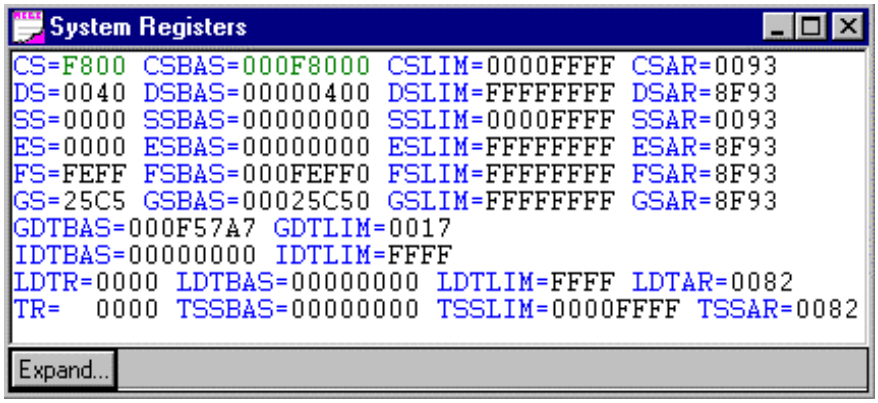
An Application Note

www.arium.com

Many developers are unfamiliar with a very important set of registers that play a crucial role in memory access. These registers are sometimes referred to as "descriptor cache" or "hidden" registers. They are accessible and modifiable only when using an in-circuit emulator (ICE) such as those produced by American Arium. This application note will explain how these registers are the true basis for forming linear addresses rather than the segment registers, even in real mode.

When code execution causes a descriptor table lookup, the processor goes into the descriptor table once to access the descriptor's base, limit and access rights. A group of three hidden registers linked to each segment register retains this information. The processor will not need to access this table entry again until a segment change is made.

The following figure shows an example of a System Registers window from an American Arium ICE. Note that it displays the descriptor cache for all six segment registers. The remainder of this application note will discuss the code descriptor cache (i.e., CSBAS, CSLIM, and CSAR), but this information generally applies to all six descriptor caches.



The linear address where code is accessed is determined by the CSBAS register. CS simply serves to convey the information into CSBAS. For example, if a real mode program executes a far call that loads a value of F800 into CS, a value of 000F8000 is loaded into CSBAS. The linear address is derived by adding CSBAS to EIP.

These descriptor cache registers also explain why the reset vector is FFFFFFFO even though CS is F000 and EIP is 0000FFF0. The reset vector is produced by adding CSBAS (FFFF0000) to EIP (0000FFF0). Since the address is derived in this manner, the reset value in CS has no effect. The CS register is initialized to F000 at reset solely for software compatibility with legacy processors.

When entering protected mode, system software must perform a far jump that loads CS to reference the appropriate descriptor in the GDT. This causes the processor to access the code descriptor and cache the base, limit, and access rights in CSBAS, CSLIM, and CSAR. The values remain in these hidden registers until execution changes context by loading another code descriptor.

Modifying a segment register (i.e., a segment selector) manually does not have the same effect as when it is modified by program execution. For instance, CSBAS, CSLIM, and CSAR are not automatically changed when CS is modified using an ICE. In most cases, all of these registers will need to be changed to produce the desired effect.

14281 Chambers Road
Tustin, CA 92780
Voice: 714-731-1661
Fax: 714-731-6344
Web: www.arium.com
E-mail: info@arium.com